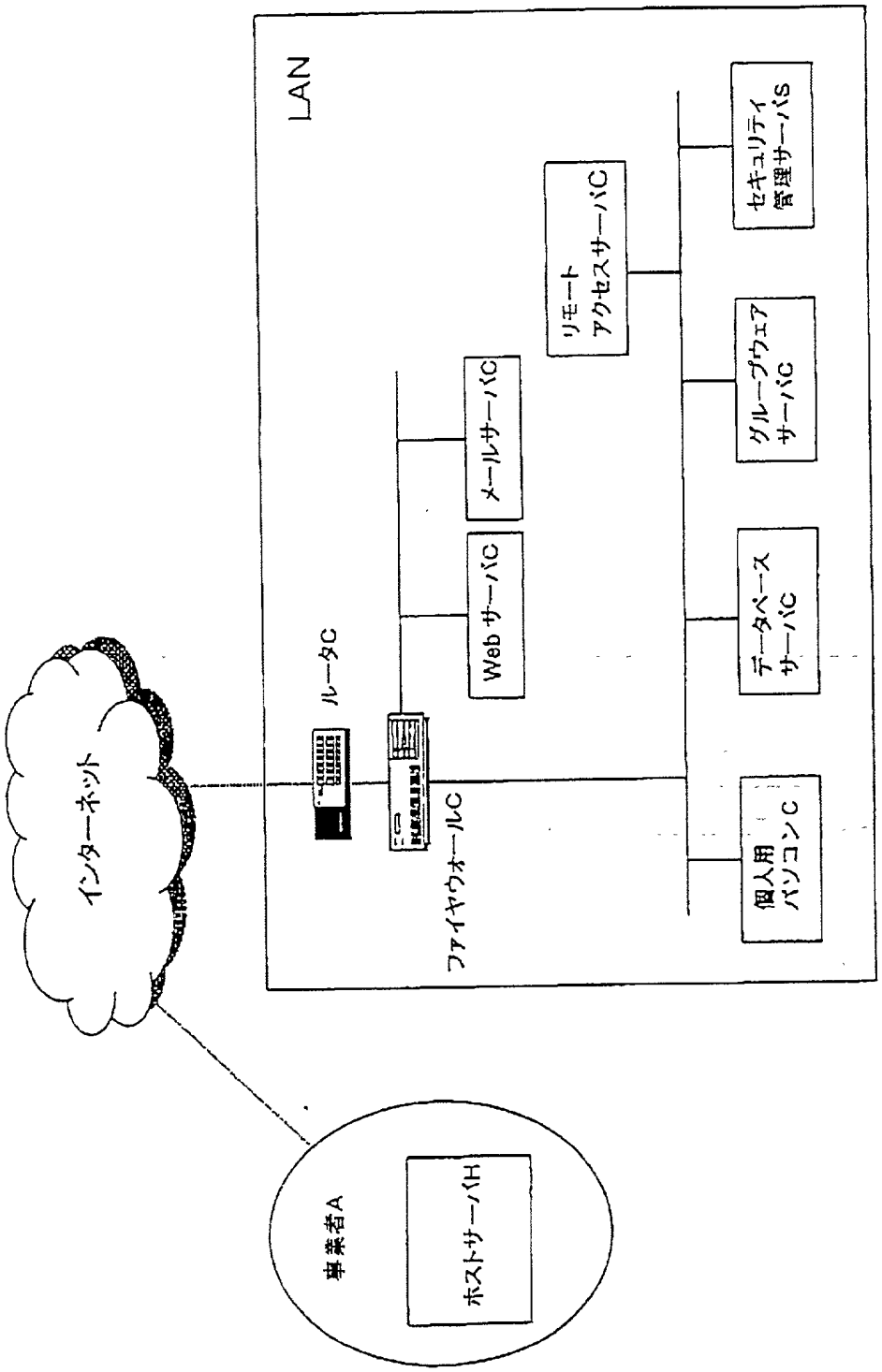
提出日　平成１３年　６月　５日

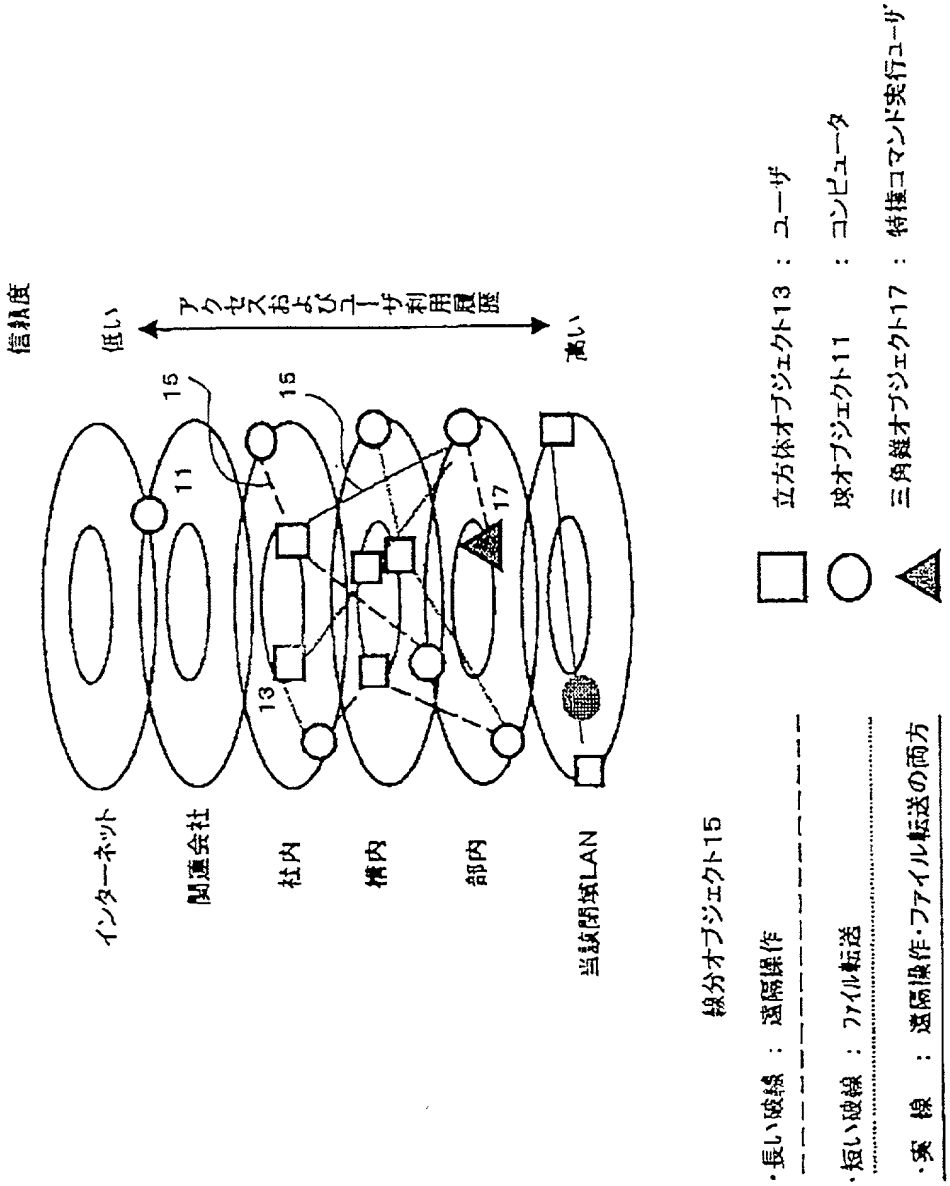
整理番号＝ＩＤ０１０２２０

【書類名】　　図面

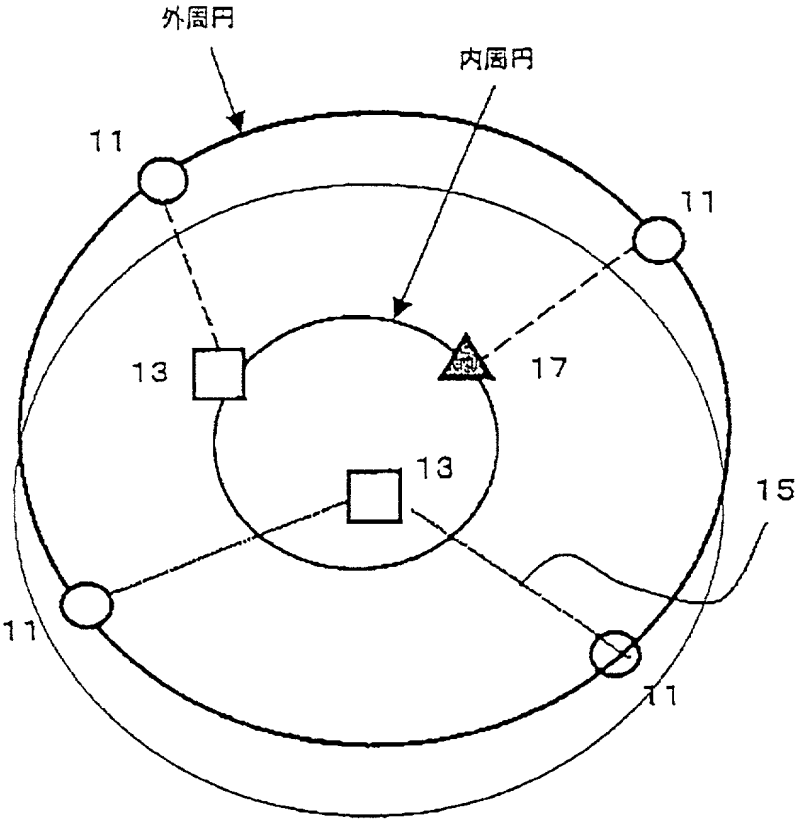
【図１】



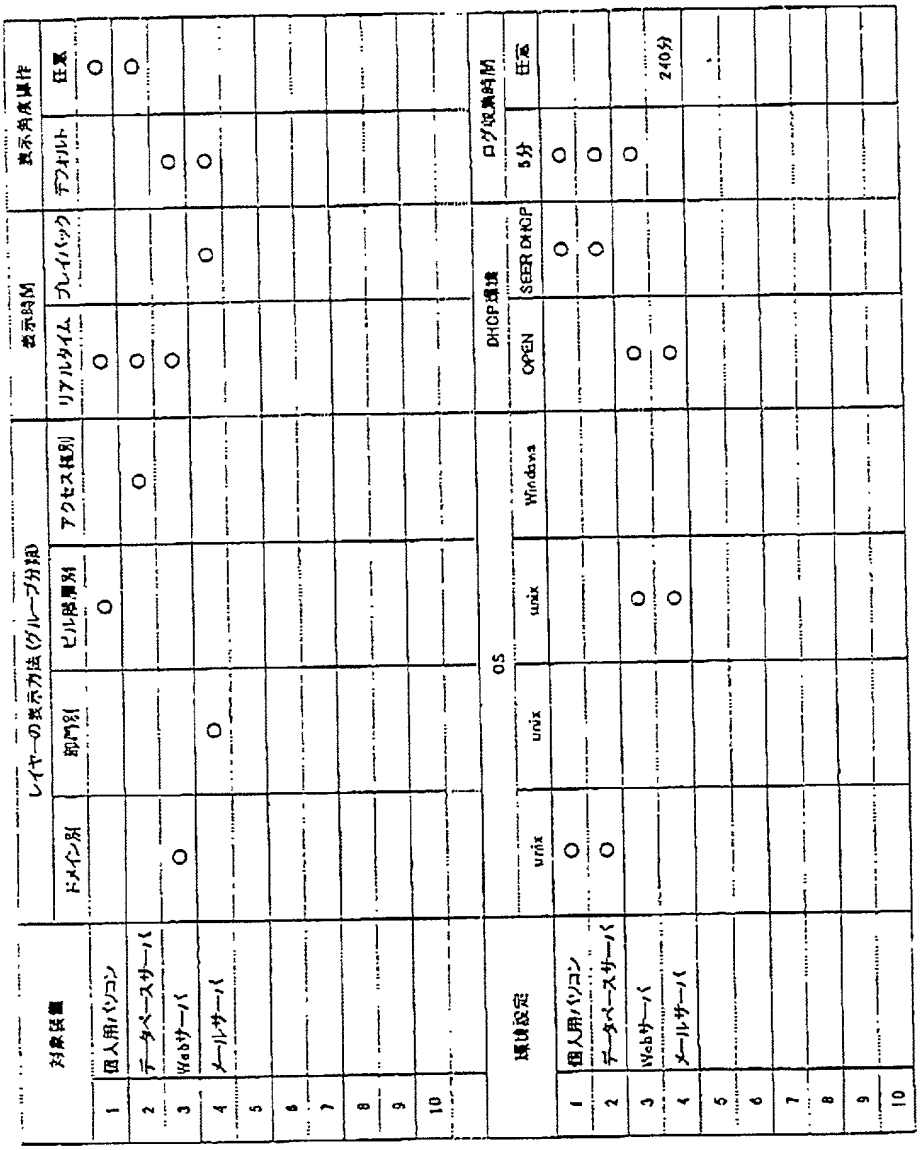
【図２】


信頼度
低い
アクセスおよびユーザ利用履歴
高い
15
15
11
13
17
インターネット
関連会社
社内
構内
部内
当該閉域LAN
線分オブジェクト15
・長い破線　：遠隔操作
・短い破線　：ファイル転送
・実線　：遠隔操作・ファイル転送の両方
立方体オブジェクト13　：ユーザ
球オブジェクト11　：コンピュータ
三角錐オブジェクト17　：特権コマンド実行ユーザ

【図３】



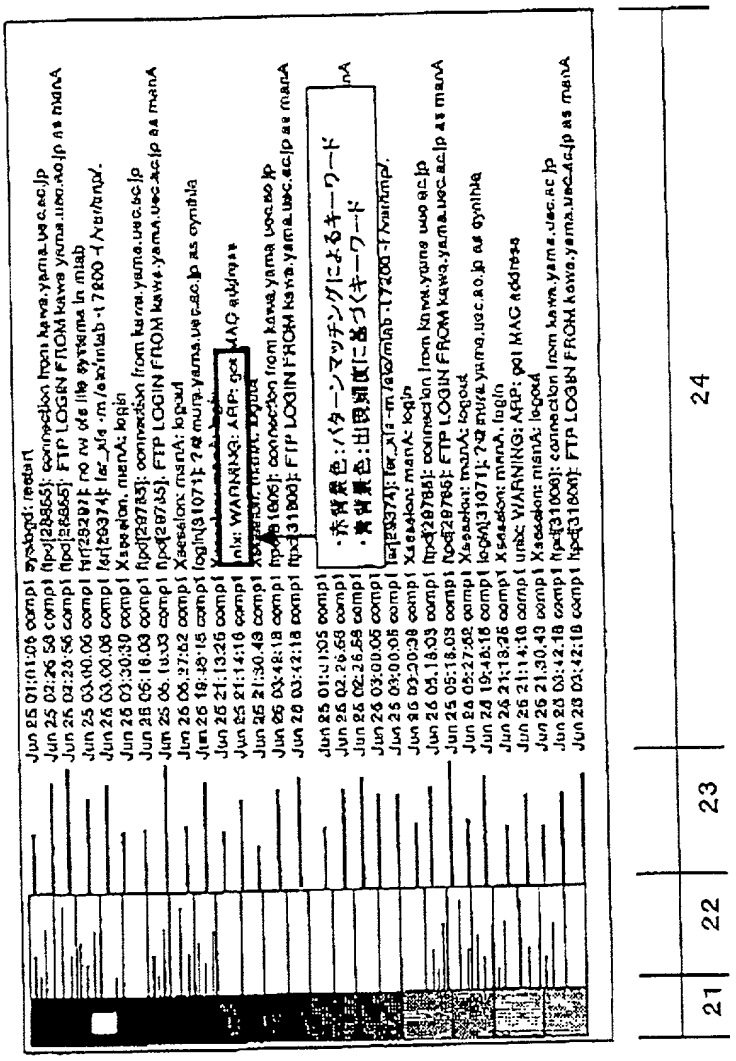
【図４】



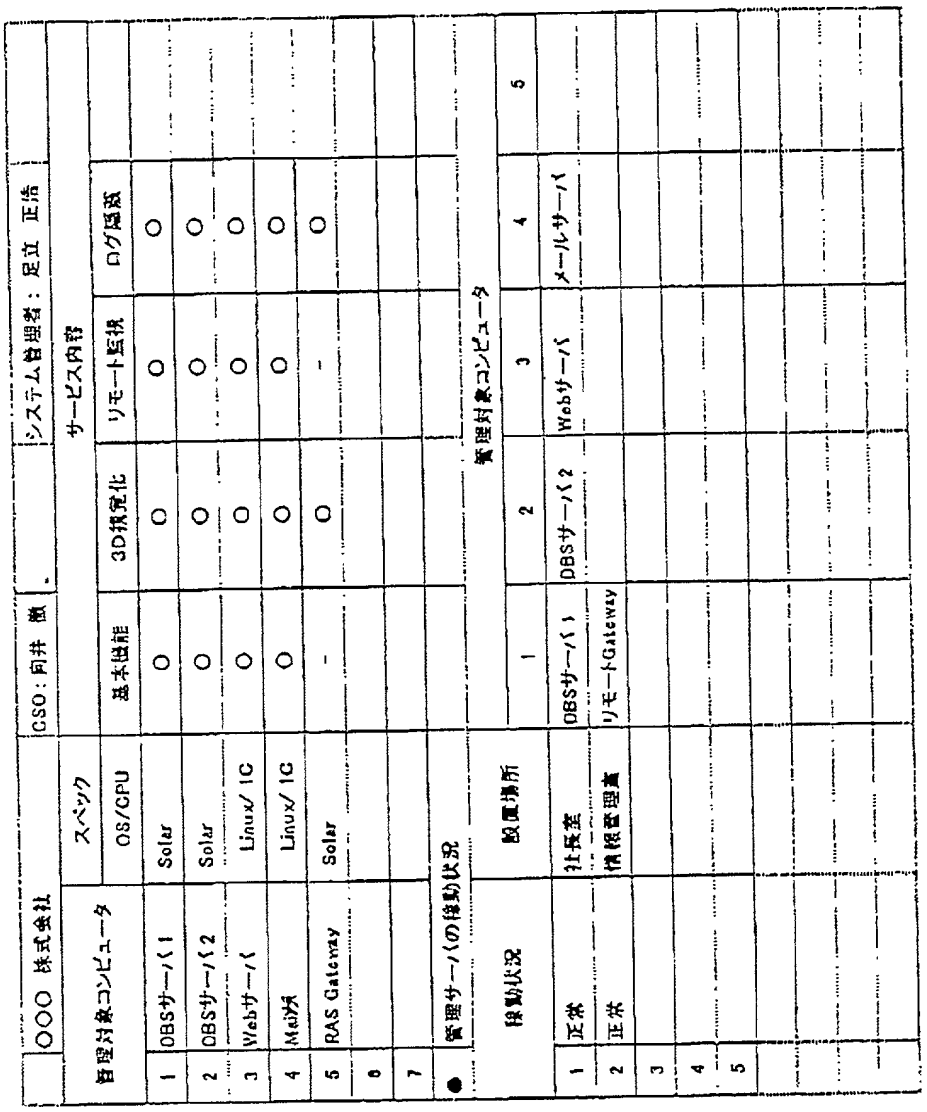
	対象装置	レイヤーの表示方法(グループ分け)				表示時M		表示角度操作	
		ドメイン別	部門別	ビル設置別	アクセス規則別	リアルタイム	プレイバック	デフォルト	任意
1	個人用パソコン			○		○			○
2	データベースサーバ				○	○			○
3	Webサーバ	○				○		○	
4	メールサーバ		○				○	○	
5									
6									
7									
8									
9									
10									

	環境設定	OS			DHCP環境		ログ収集時間	
		unix	unix	Windows	OPEN	SEER DHCP	5分	任意
1	個人用パソコン	○				○	○	
2	データベースサーバ	○				○	○	
3	Webサーバ				○		○	240分
4	メールサーバ				○			
5								
6								
7								
8								
9								
10								

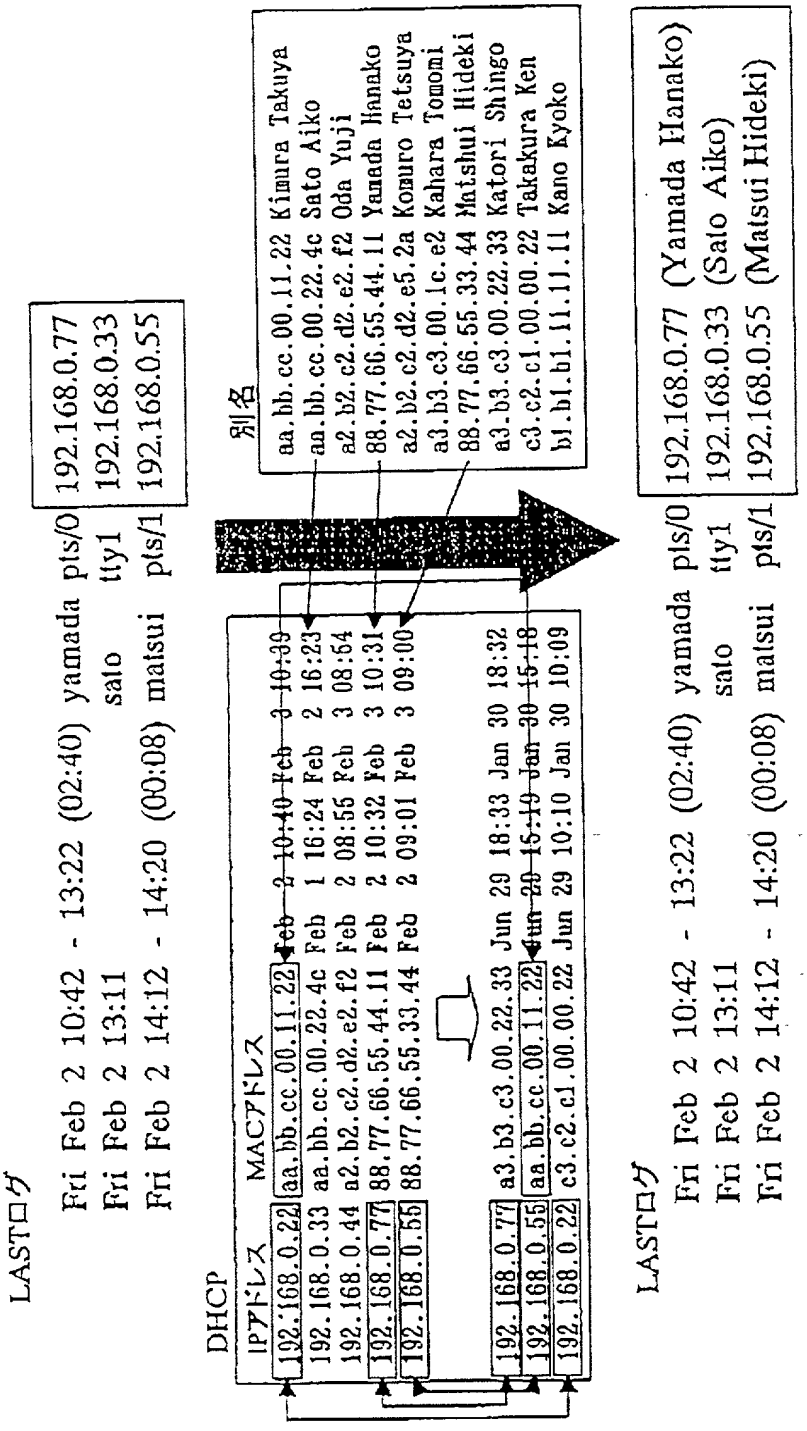
【図５】



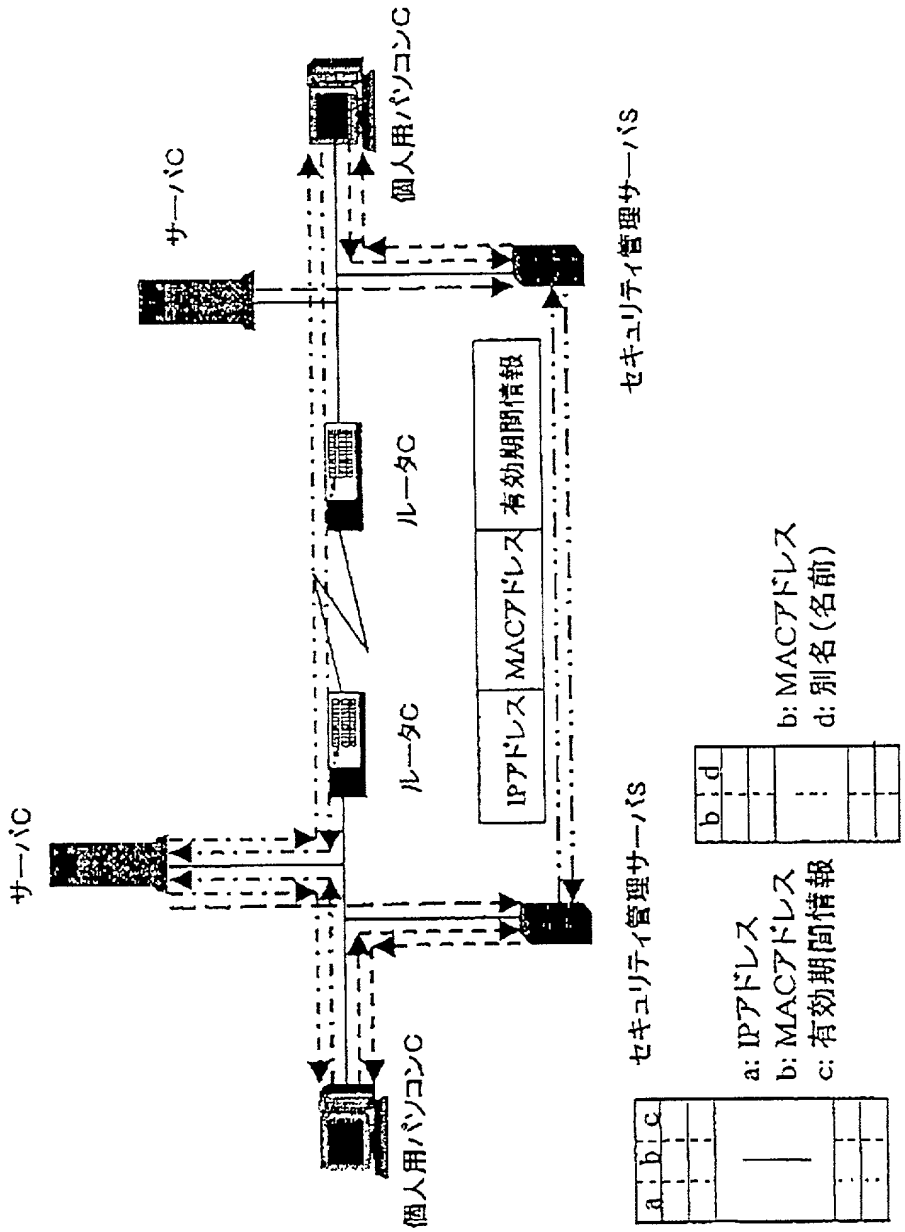
【図６】


○○○ 株式会社
CSO：向井 徹
システム管理者：足立 正浩
管理対象コンピュータ
スペック
OS/CPU
サービス内容
基本機能
3D視覚化
リモート監視
ログ監視
1 OBSサーバ1 Solar
2 OBSサーバ2 Solar
3 Webサーバ Linux/ IC
4 MailSV Linux/ IC
5 RAS Gateway Solar
6
7
● 管理サーバの稼動状況
稼動状況
設置場所
管理対象コンピュータ
1 正常 社長室 OBSサーバ1
2 正常 情報管理室 リモートGateway
3
4
5
1
2 OBSサーバ2
3 Webサーバ
4 メールサーバ
5

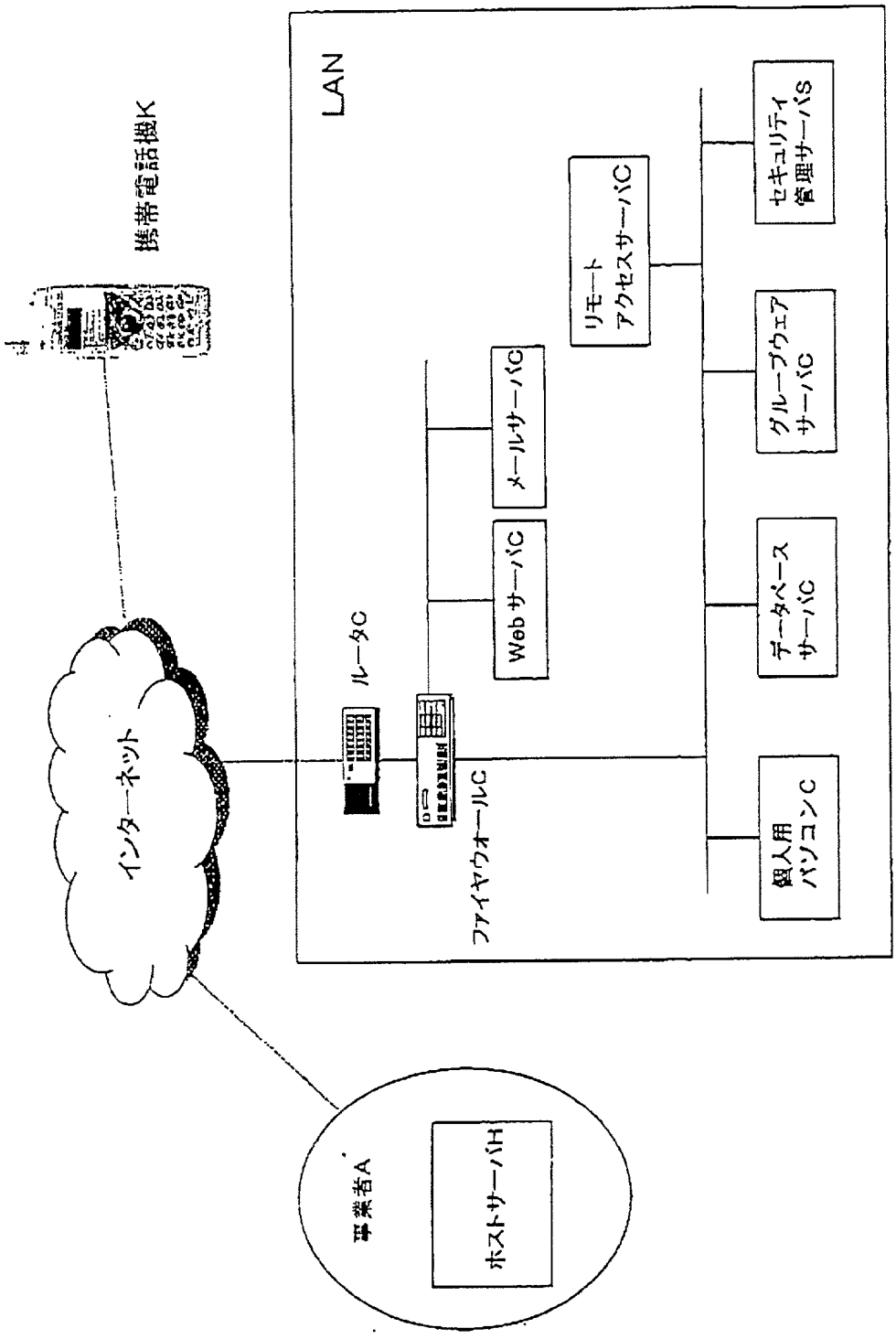
【図７】


LASTログ
Fri Feb 2 10:42 - 13:22 (02:40) yamada pts/0
Fri Feb 2 13:11 sato tty1
Fri Feb 2 14:12 - 14:20 (00:08) matsui pts/1
192.168.0.77
192.168.0.33
192.168.0.55
別名
aa.bb.cc.00.11.22 Kimura Takuya
aa.bb.cc.00.22.4c Sato Aiko
a2.b2.c2.d2.e2.f2 Oda Yuji
88.77.66.55.44.11 Yamada Hanako
a2.b2.c2.d2.e5.2a Komuro Tetsuya
a3.b3.c3.00.1c.e2 Kahara Tomomi
88.77.66.55.33.44 Matshui Hideki
a3.b3.c3.00.22.33 Katori Shingo
c3.c2.c1.00.00.22 Takakura Ken
b1.b1.b1.11.11.11 Kano Kyoko
DHCP
IPアドレス
MACアドレス
192.168.0.22 aa.bb.cc.00.11.22 Feb 2 10:40 Feb 3 10:39
192.168.0.33 aa.bb.cc.00.22.4c Feb 1 16:24 Feb 2 16:23
192.168.0.44 a2.b2.c2.d2.e2.f2 Feb 2 08:55 Feb 3 08:54
192.168.0.77 88.77.66.55.44.11 Feb 2 10:32 Feb 3 10:31
192.168.0.55 88.77.66.55.33.44 Feb 2 09:01 Feb 3 09:00
192.168.0.77 a3.b3.c3.00.22.33 Jun 29 18:33 Jun 30 18:32
192.168.0.55 aa.bb.cc.00.11.22 Jun 20 15:10 Jun 30 15:18
192.168.0.22 c3.c2.c1.00.00.22 Jun 29 10:10 Jan 30 10:09
LASTログ
Fri Feb 2 10:42 - 13:22 (02:40) yamada pts/0
Fri Feb 2 13:11 sato tty1
Fri Feb 2 14:12 - 14:20 (00:08) matsui pts/1
192.168.0.77 (Yamada Hanako)
192.168.0.33 (Sato Aiko)
192.168.0.55 (Matsui Hideki)

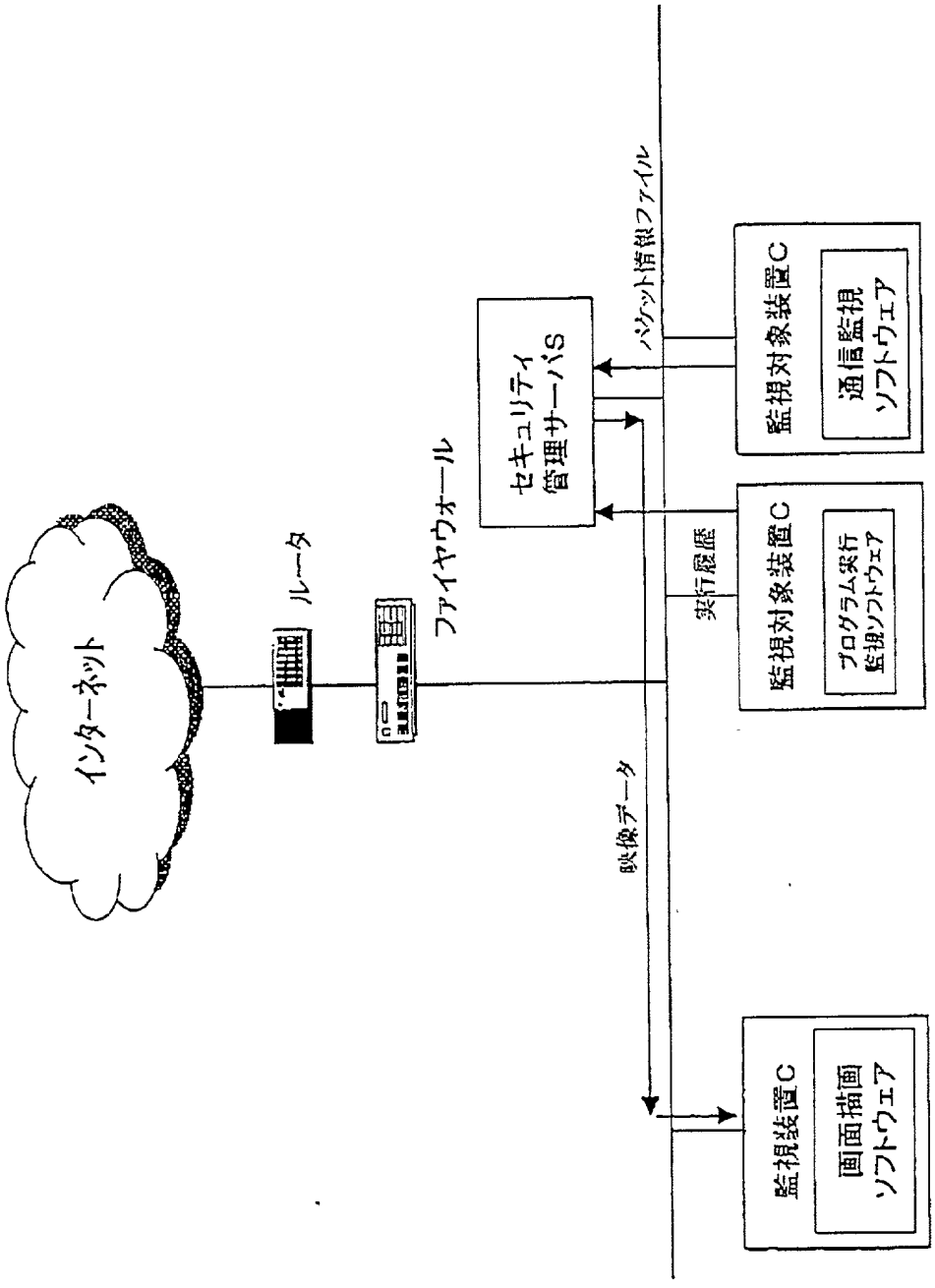
【図８】


サーバC
個人用パソコンC
ルータC
ルータC
サーバC
個人用パソコンC
IPアドレス
MACアドレス
有効期間情報
セキュリティ管理サーバS
セキュリティ管理サーバS
a: IPアドレス
b: MACアドレス
c: 有効期間情報
b: MACアドレス
d: 別名(名前)

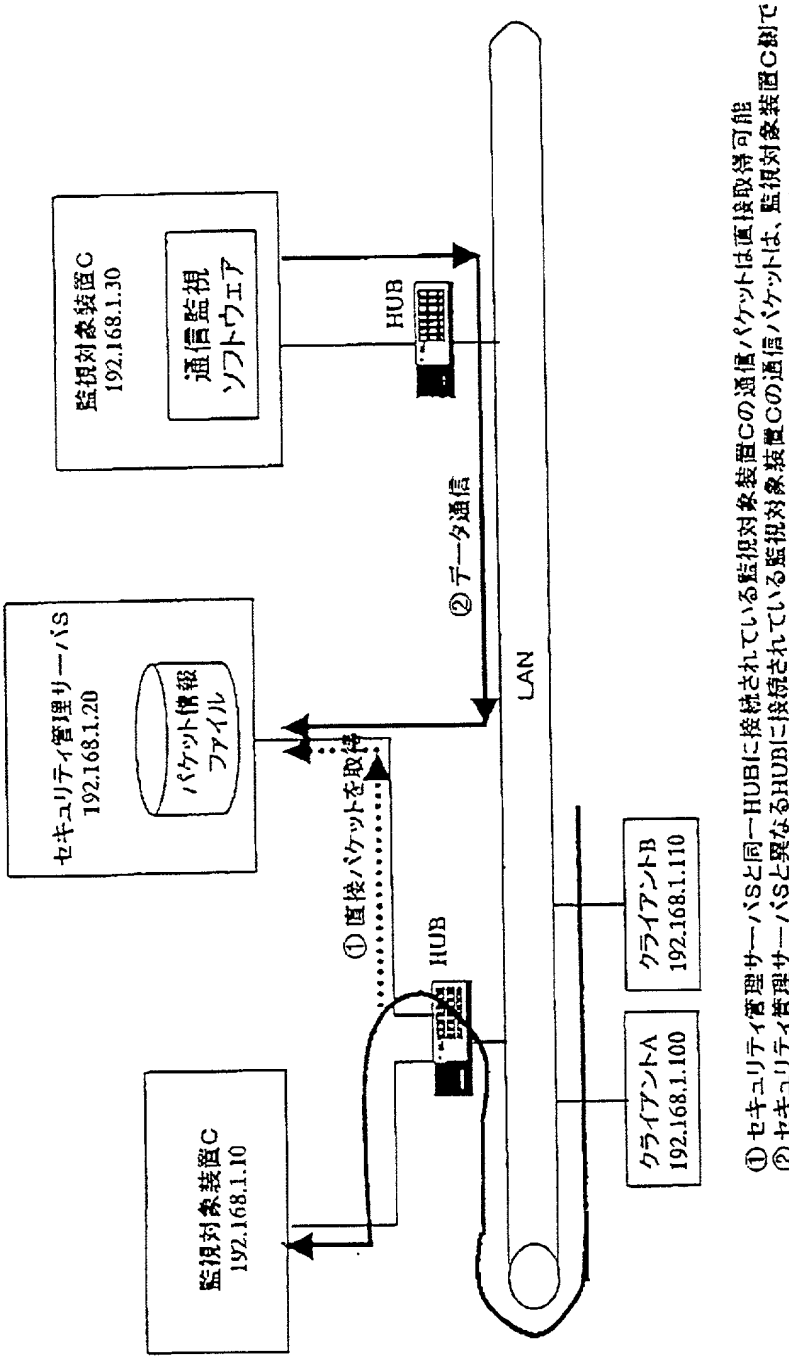
【図９】


携帯電話機K
インターネット
LAN
ルータC
ファイヤウォールC
Webサーバ
メールサーバ
リモート
アクセスサーバC
セキュリティ
管理サーバS
グループウェア
サーバC
データベース
サーバC
個人用
パソコンC
事業者A
ホストサーバH

【図１０】


インターネット
ルータ
ファイヤウォール
セキュリティ
管理サーバS
パケット情報ファイル
監視対象装置C
通信監視
ソフトウェア
実行履歴
監視対象装置C
プログラム実行
監視ソフトウェア
映像データ
監視装置C
画面描画
ソフトウェア

【図１１】



①セキュリティ管理サーバSと同一HUBに接続されている監視対象装置Cの通信パケットは直接取得可能
②セキュリティ管理サーバSと異なるHUBに接続されている監視対象装置Cの通信パケットは、監視対象装置C経由で
当該記憶しておき、これをLAN経由のデータ通信により適宜セキュリティ管理サーバSに集信する。

【図１２】

パケット情報ファイルのデータフォーマット

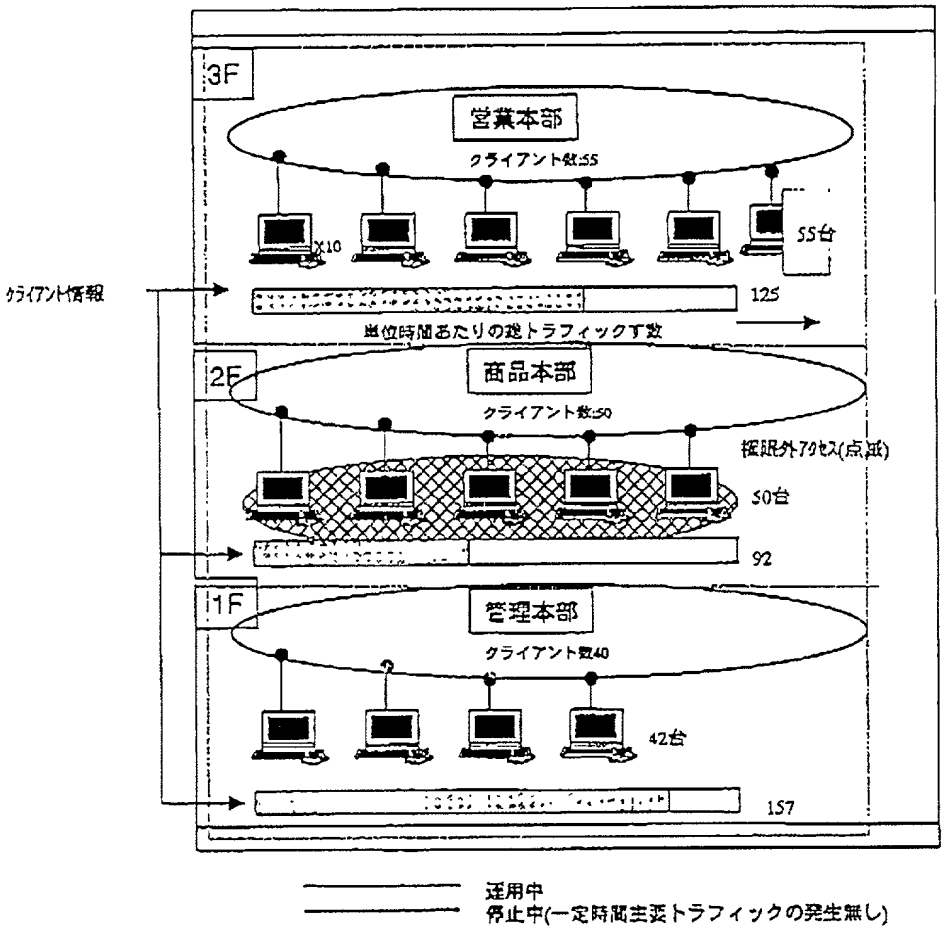
フィールド名	説明
time	収集時間(サーバー時間)
btFlags	フラグ　0:IN 1:OUT (サーバーから見て) 2:SMB(共有ファイルアクセス等)
wLength	パケットのオリジナル長
mwMac	クライアントMACアドレス
dwIPAddr	クライアントIPアドレス
wPort	サーバーポート番号
btDataLength	パケットの可変データ部分の長さ　(0から255)
btData[256]	256パケットの可変データ(可変長)

【図１３】

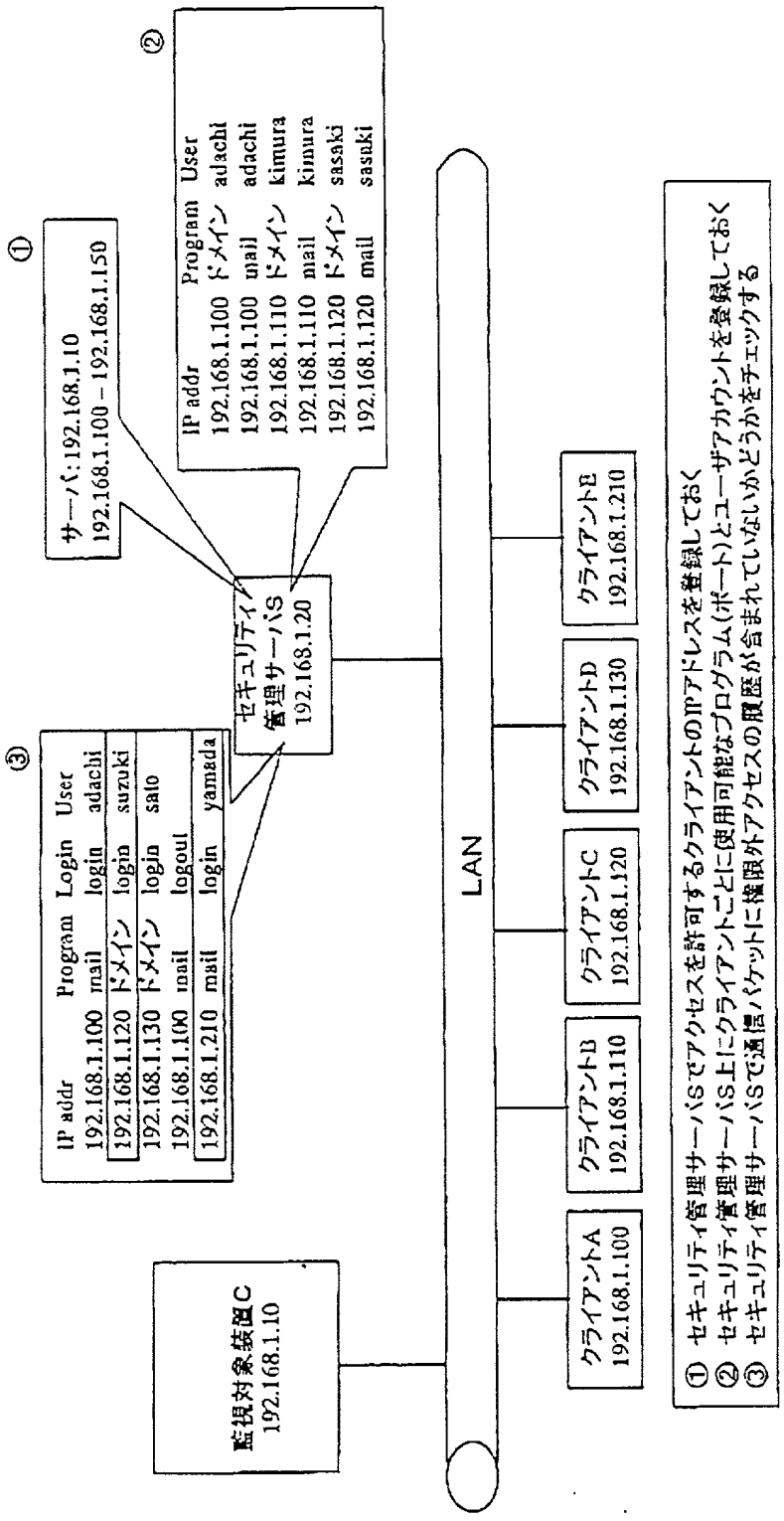
視覚化基礎データ

フィールド名	説明
time	収集時間(セキュリティ管理サーバでの時間)
wServerID	監視対象サーバー識別子
wType	パケットのタイプ (01:Login...65:Mail...)
mwMac	クライアントMACアドレス
dwIPAddr	クライアントIPアドレス
wOriginalLength	パケットのオリジナル長
btData[256]	256パケットのタイプ別文字データ (Login:UserID/Mail:from.to...)

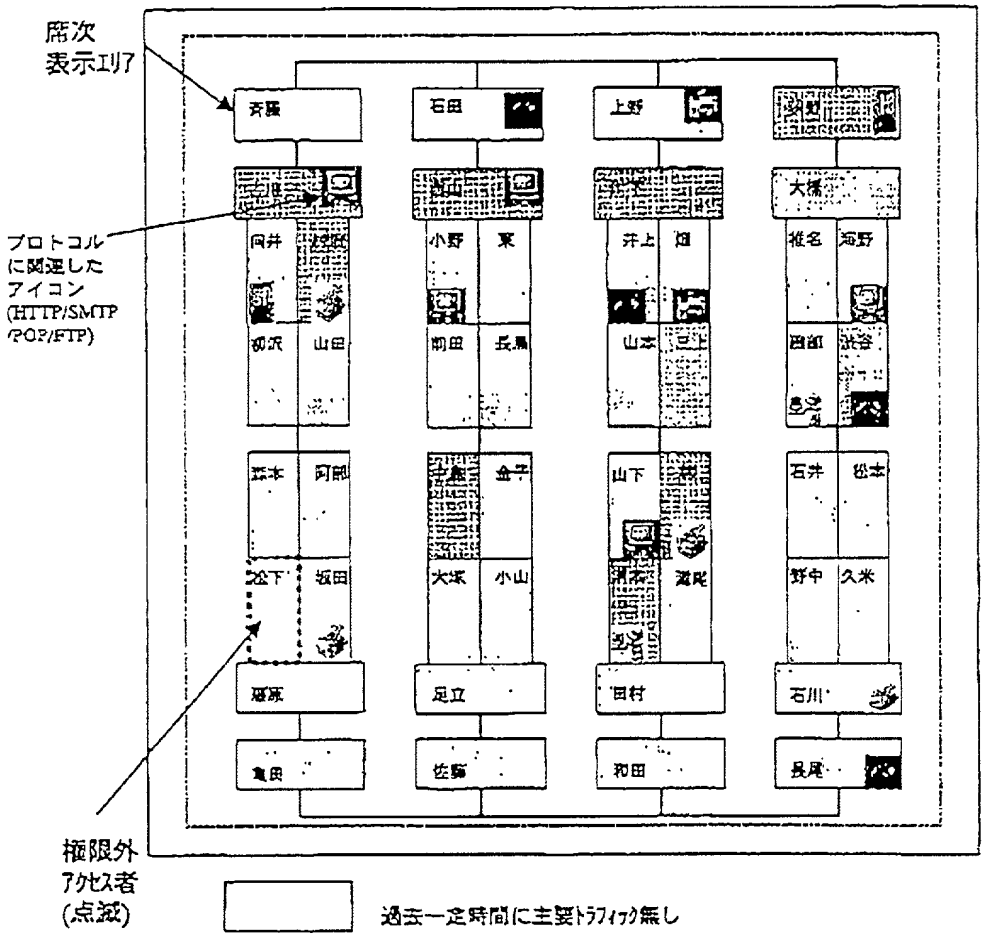
【図１４】


3F
営業本部
クライアント数:55
X10
55台
クライアント情報
125
単位時間あたりの総トラフィック数
2F
商品本部
クライアント数:50
不正アクセス(点滅)
50台
92
1F
管理本部
クライアント数40
42台
157
運用中
停止中(一定時間主要トラフィックの発生無し)

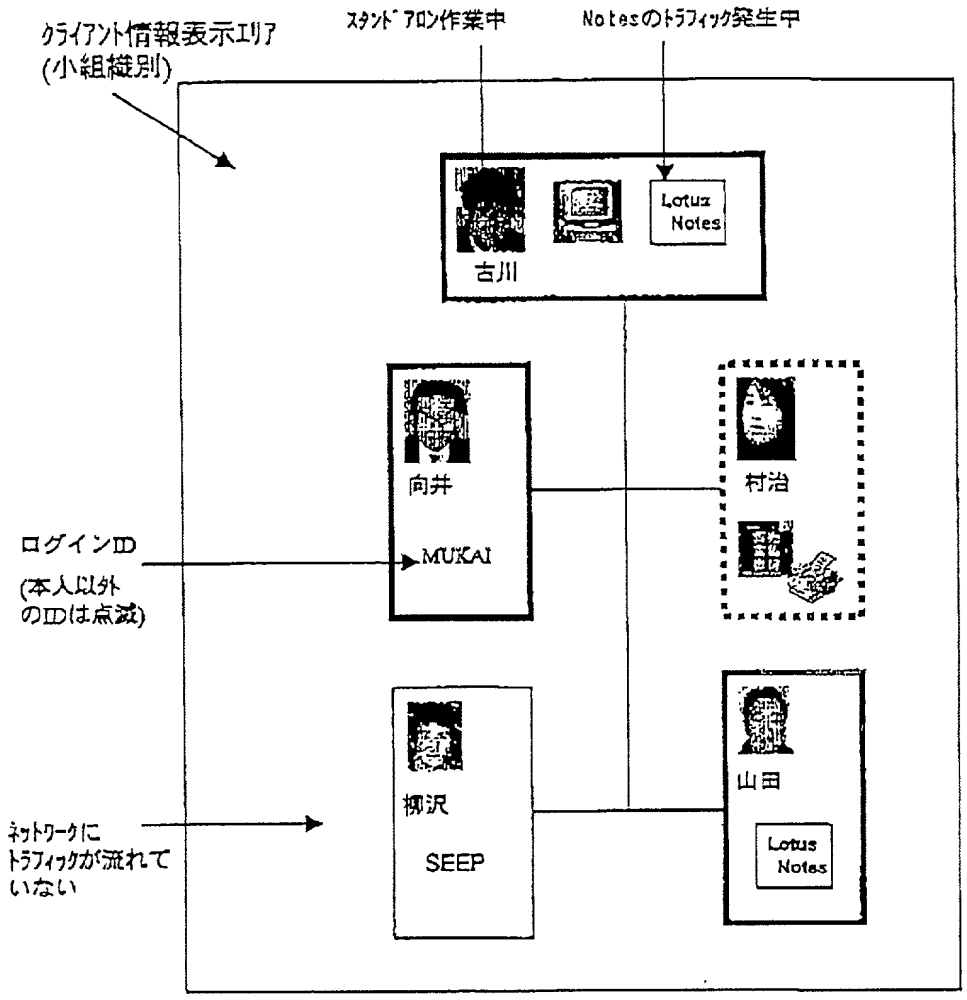
【図１５】


①
サーバ：192.168.1.10
192.168.1.100 – 192.168.1.150
②
IP addr Program User
192.168.1.100 ドメイン adachi
192.168.1.100 mail adachi
192.168.1.110 ドメイン kimura
192.168.1.110 mail kimura
192.168.1.120 ドメイン sasaki
192.168.1.120 mail sasaki
③
IP addr Program Login User
192.168.1.100 mail login adachi
192.168.1.120 ドメイン login suzuki
192.168.1.130 ドメイン login sato
192.168.1.100 mail logout
192.168.1.210 mail login yamada
セキュリティ管理サーバS
192.168.1.20
LAN
監視対象装置C
192.168.1.10
クライアントA
192.168.1.100
クライアントB
192.168.1.110
クライアントC
192.168.1.120
クライアントD
192.168.1.130
クライアントE
192.168.1.210
① セキュリティ管理サーバSでアクセスを許可するクライアントのIPアドレスを登録しておく
② セキュリティ管理サーバS上にクライアントごとに使用可能なプログラム(ポート)とユーザアカウントを登録しておく
③ セキュリティ管理サーバSで通信パケットに権限外アクセスの履歴が含まれていないかどうかをチェックする

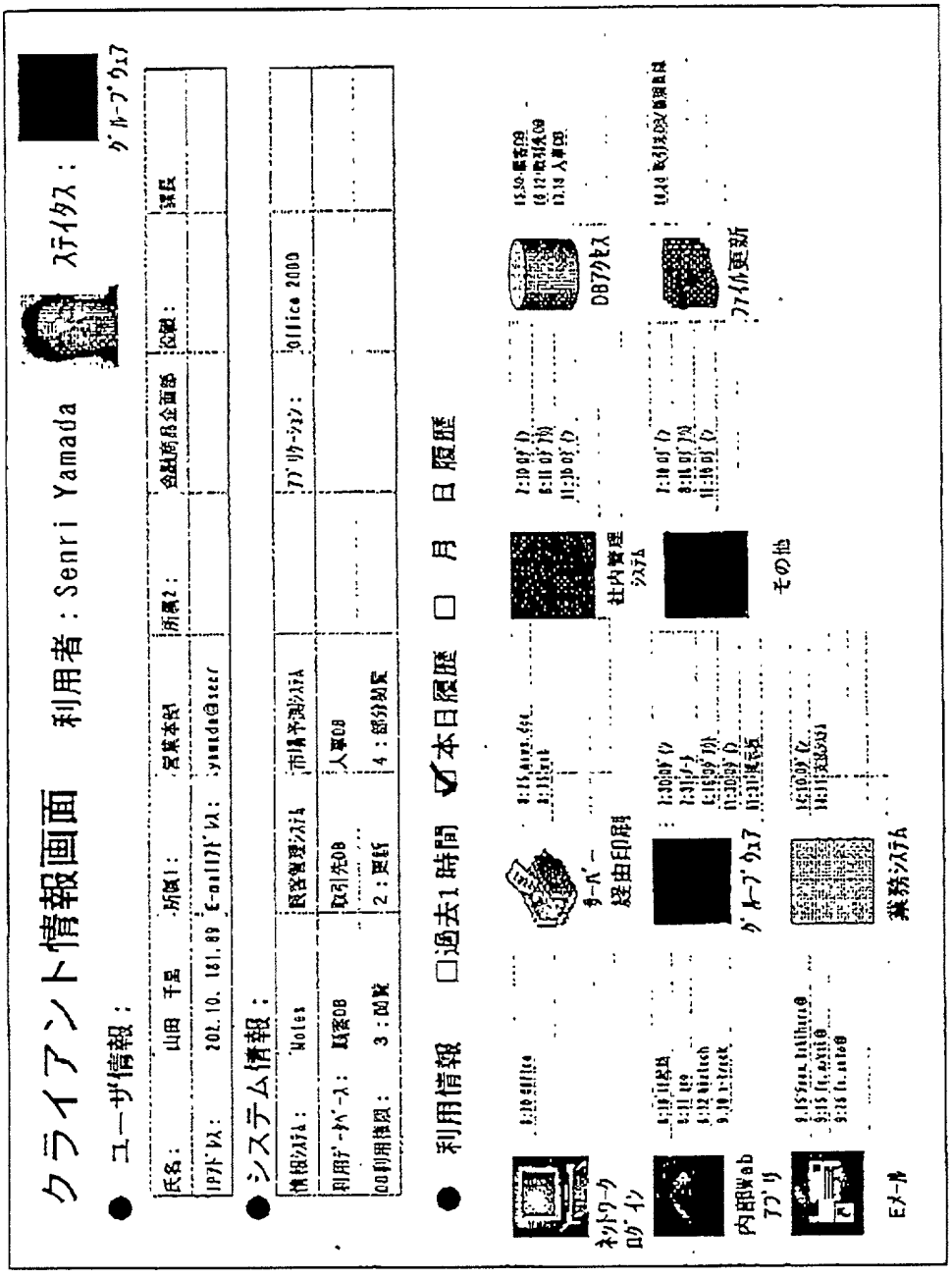
【図１６】


席次
表示エリア
プロトコル
に関連した
アイコン
(HTTP/SMTP
/POP/FTP)
権限外
アクセス者
(点滅)
過去一定時間に主要トラフィック無し

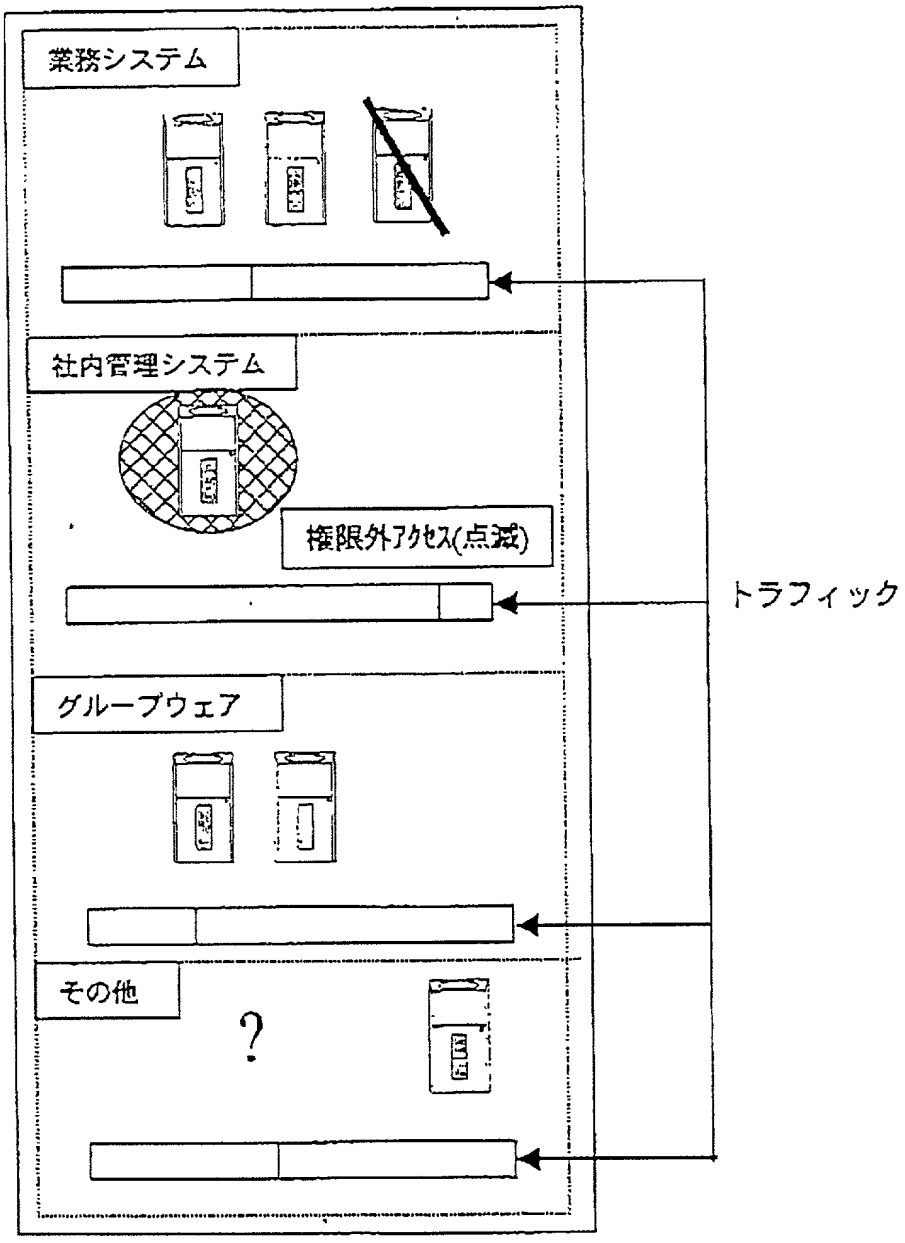
【図１７】


ｸﾗｲｱﾝﾄ情報表示ｴﾘｱ
(小組織別)
ｽﾀﾝﾄﾞｱﾛﾝ作業中
Notesのﾄﾗﾌｨｯｸ発生中
Lotus Notes
古川
向井
MUKAI
村治
ログインID
(本人以外のIDは点滅)
柳沢
SEEP
山田
Lotus Notes
ﾈｯﾄﾜｰｸにﾄﾗﾌｨｯｸが流れていない

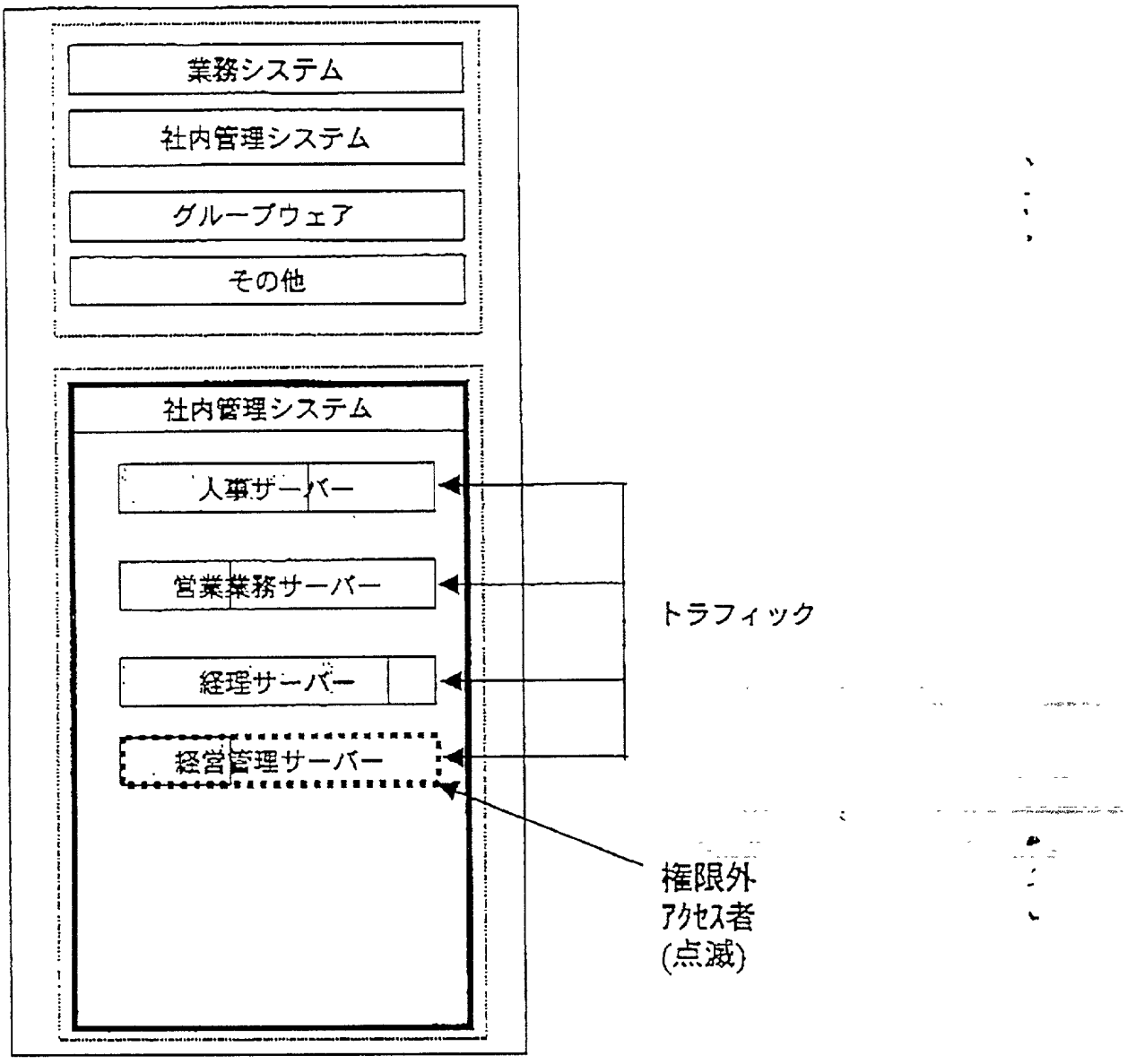
【図１８】


クライアント情報画面
利用者：Senri Yamada
ステイタス：
グループウェア
● ユーザ情報：
氏名：　山田　千里　所属1：　営業本部　所属2：　企画部企画部　役職：　課長
IPアドレス：　202.10.181.89　E-mailアドレス：　yamada@user
● システム情報：
情報システム：　Notes　販売管理システム　市場予測システム　アプリケーション：　Office 2000
利用データベース：　顧客DB　取引先DB　人事DB
DB利用権限：　3：閲覧　2：更新　4：部分処理
● 利用情報　□過去1時間　☑本日履歴　□　月　日履歴
ネットワークログイン
メール経由印刷
社内管理システム
DBアクセス
内部Webアプリ
グループウェア
その他
ファイル更新
業務システム
Eメール

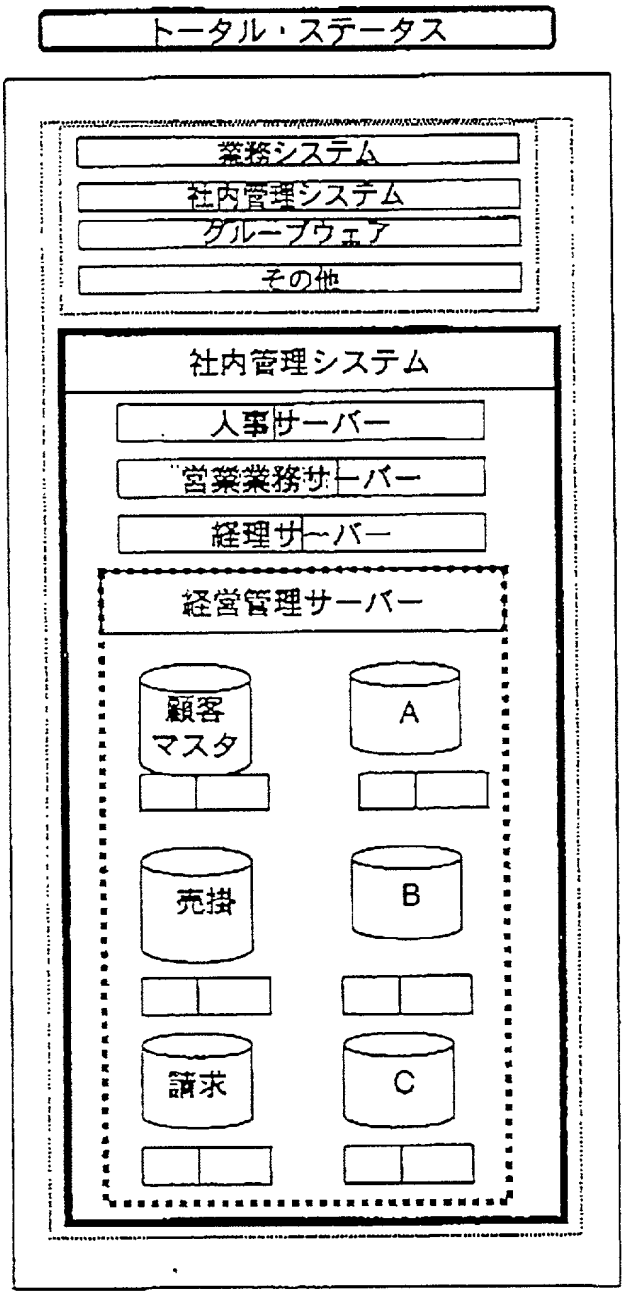
【図１９】



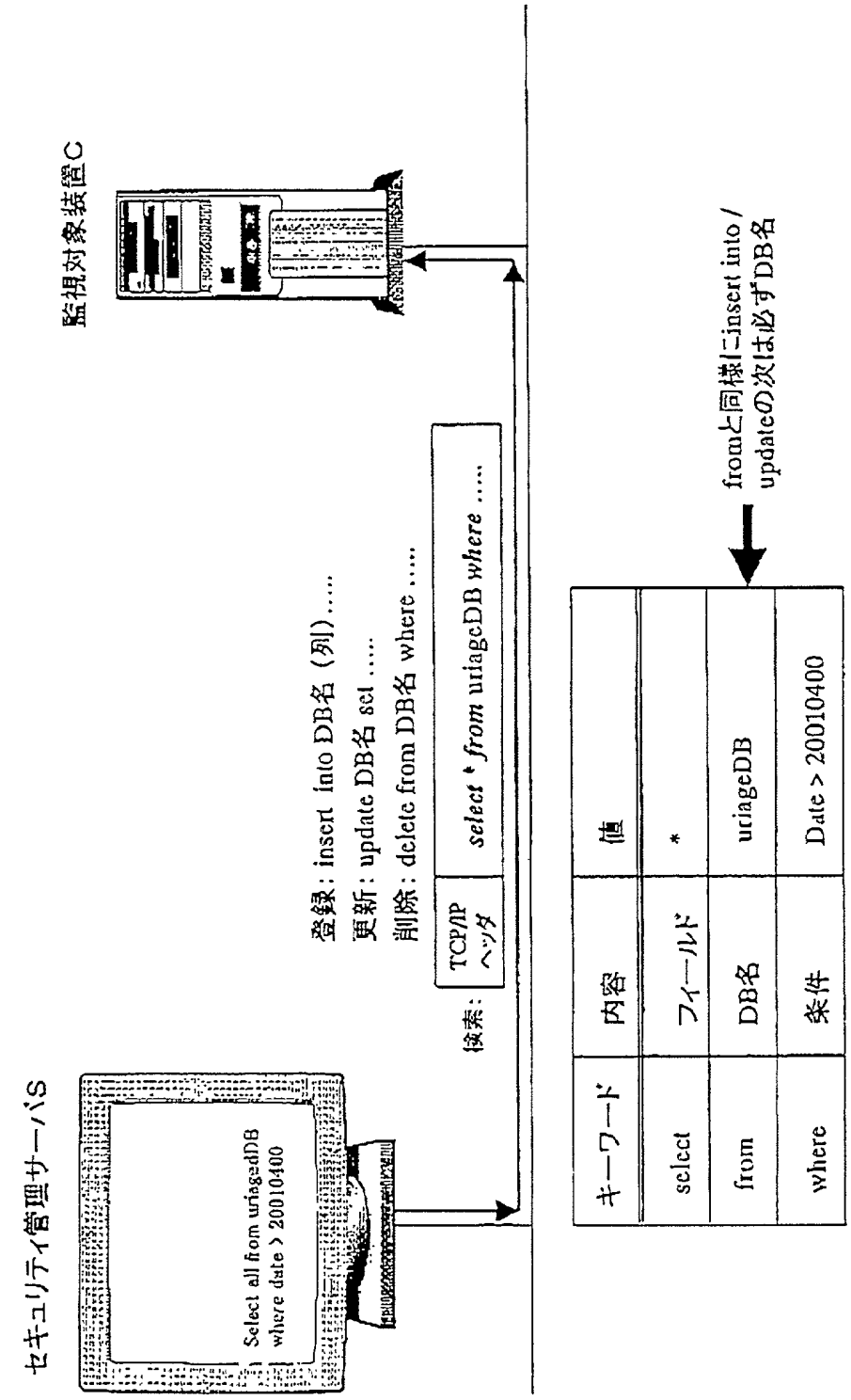
【図２０】


業務システム
社内管理システム
グループウェア
その他
社内管理システム
人事サーバー
営業業務サーバー
経理サーバー
経営管理サーバー
トラフィック
権限外
ｱｸｾｽ者
(点滅)

【図２１】


トータル・ステータス
業務システム
社内管理システム
グループウェア
その他
社内管理システム
人事サーバー
営業業務サーバー
経理サーバー
経営管理サーバー
顧客マスタ
A
売掛
B
請求
C

【図２２】


セキュリティ管理サーバS
Select all from uriageDB
where date > 20010400
検索：
TCP/IP ヘッダ
select * from uriageDB where .....
登録：insert into DB名 (列).....
更新：update DB名 set .....
削除：delete from DB名 where .....
監視対象装置C
fromと同様にinsert into / updateの次は必ずDB名
キーワード
内容
値
select
フィールド
*
from
DB名
uriageDB
where
条件
Date > 20010400

提出日　平成１３年　６月　５日

【書類名】　　要約書

【要約】

【課題】　ＬＡＮにおける各種のセキュリティサービスを提供するセキュリティ管理サーバおよびこれと連携して動作するホストサーバを提供する。

【解決手段】　インターネットなどの外部のネットワークに接続するＬＡＮ内に、ＬＡＮ内で稼働する各種監視対象装置Ｃ内で管理されている各種のログ情報を収集する機能、収集したログ情報からＬＡＮのセキュリティ管理に有用な情報を抽出してこれを人が利用しやすい形態に視覚化した映像を生成する機能、前記映像を他の監視装置Ｃに送信する機能を備えたセキュリティ管理サーバＳを設置する。また、セキュリティ管理サーバＳは、外部のネットワークで稼働するホストサーバＨと連携して各種のセキュリティサービスを提供する。

【選択図】　　図１